BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11203128 A**

(43) Date of publication of application: **30 . 07 . 99**

(51) Int. Cl **G06F 9/06**
G06F 12/14
G09C 1/00
H04L 9/10

(21) Application number: **10003366**

(22) Date of filing: **09 . 01 . 98**

(71) Applicant: **CANON INC**

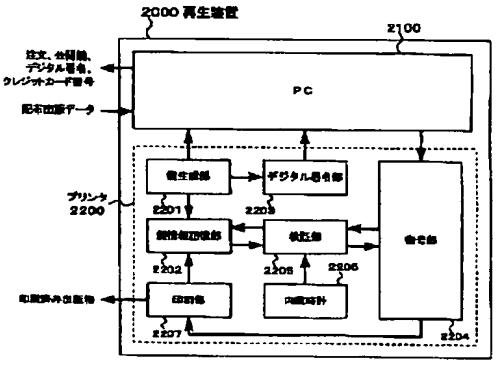
(72) Inventor: **HOSHINO HITOSHI**

(54) **DIGITAL SOFTWARE DISTRIBUTION SYSTEM, TERMINAL AND RECORDING MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To effectively prevent illegal use where a user holding enciphered distribution digital softwares, repeatedly utilizes them by using a decoder.

SOLUTION: A reproducing device 2000 which receives software is internally provided with a key information storing part 2202 which stores a decode key, an decoding part 2204 which decodes enciphered distribution software with the decode key and an authenticating part 2205 which discards a stored decode key in a decided timing and prevents decoding after the decode key is discarded by opening a key of cryptograph to the public between a code key and the key of cryptograph which are produced by a software receiving end, also storing the decode key at the receiving end and later discarding it in a decided timing so that the distribution software can be decoded and utilized only while the decode key is stored at the receiving end.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－203128

(43)公開日　平成11年(1999)７月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｚ
	12/14	３２０		12/14	３２０Ｂ
Ｇ０９Ｃ	1/00	６２０	Ｇ０９Ｃ	1/00	６２０Ｚ
Ｈ０４Ｌ	9/10		Ｈ０４Ｌ	9/00	６２１Ａ

審査請求　未請求　請求項の数28　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－3366

(22)出願日　平成10年(1998)１月９日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　星野　仁
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

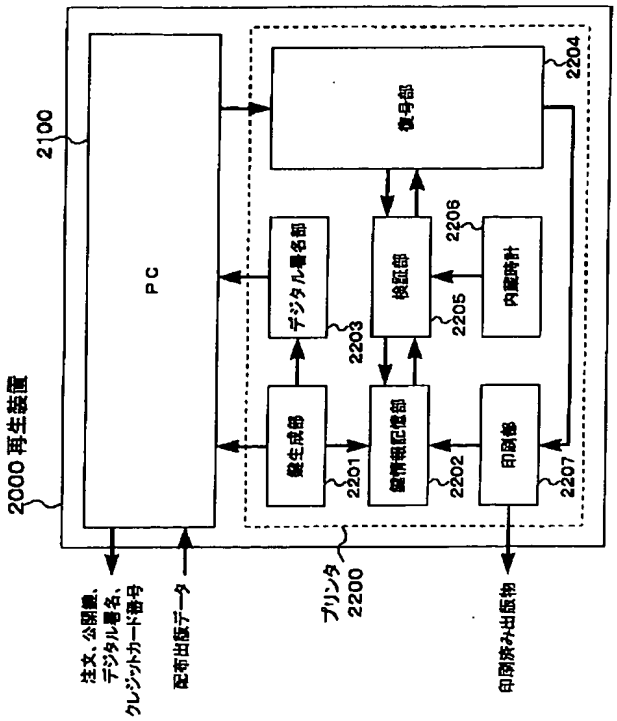
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　デジタルソフトウェア配布システム、端末装置および記録媒体

(57)【要約】

【課題】　使用者が暗号化された配布デジタルソフトウェアを保持し、復号装置を使用して繰り返し利用する不正を有効に防止できるようにする。

【解決手段】　ソフトウェアを受信する再生装置２０００内に、復号鍵を記憶する鍵情報記憶部２２０２と、暗号化された配布ソフトウェアを上記復号鍵で復号する復号部２２０４と、記憶された復号鍵を決められたタイミングで破棄するようにする検証部２２０５とを設け、ソフトウェアの受信側で生成した暗号鍵と復号鍵のうち、暗号鍵を公開するとともに復号鍵を受信側に記憶しておき、それをその後決められたタイミングで破棄するようにすることにより、復号鍵が破棄された後は復号できなくなるようにして、受信側に復号鍵が記憶されている間だけ配布ソフトウェアを復号して利用することができるようにする。



1

【特許請求の範囲】

【請求項１】　デジタルソフトウェアを配布するデジタルソフトウェア配布システムにおいて、

上記デジタルソフトウェアの受信側は少なくとも、暗号鍵およびこの暗号鍵で暗号化したデータを復号化できる復号鍵を生成する鍵生成手段と、

上記暗号鍵を外部に公開する鍵情報公開手段と、

上記復号鍵を記憶する鍵情報記憶手段と、

上記外部に公開された暗号鍵によって暗号化された配布デジタルソフトウェアを受け取り、上記記憶しておいた復号鍵で復号する復号手段と、

上記鍵情報記憶手段に記憶されている復号鍵を決められたタイミングで破棄する鍵情報破棄手段とを備え、

上記デジタルソフトウェアの配付側は少なくとも、上記公開された暗号鍵を受け取る鍵情報受信手段と、

上記受信した暗号鍵で配布するデジタルソフトウェアを暗号化する暗号化手段とを備えたことを特徴とするデジタルソフトウェア配布システム。

【請求項２】　上記鍵情報記憶手段が記憶している復号鍵を破棄するタイミングは、上記配布デジタルソフトウェアを復号し終えたことに応じて決定されることを特徴とする請求項１に記載のデジタルソフトウェア配布システム。

【請求項３】　上記デジタルソフトウェアの受信側はさらに、上記復号手段により復号された配布デジタルソフトウェアを物理的な形に再生する再生手段を備え、

上記鍵情報記憶手段が記憶している復号鍵を破棄するタイミングは、上記配布デジタルソフトウェアを物理的な形に正常に再生し終えたことに応じて決定され、再生に失敗した場合には当該再生の失敗に応じて上記復号鍵の破棄を行わないことを特徴とする請求項１に記載のデジタルソフトウェア配布システム。

【請求項４】　上記デジタルソフトウェアの受信側は、

上記復号鍵を複数個記憶する手段と、

上記複数の復号鍵毎に識別子を設定する手段と、

上記設定した復号鍵の識別子を記憶する手段と、

上記識別子を外部に公開する手段と、

上記識別子から対応する復号鍵を求める手段とを備え、

上記デジタルソフトウェアの配付側は、上記公開された識別子を受け取る手段と、

上記受信した識別子を配付デジタルソフトウェアに添付する手段とを備え、

上記デジタルソフトウェアの受信側は、上記配付デジタルソフトウェアに添付された識別子から対応する復号鍵を求め、この求めた復号鍵によって上記配付デジタルソフトウェアの復号を行うことを特徴とする請求項１～３の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項５】　上記デジタルソフトウェアの配付側は、上記デジタルソフトウェアの使用条件情報を上記デジタルソフトウェアに添付する手段を備え、

2

上記デジタルソフトウェアの受信側は、上記配付デジタルソフトウェアに添付された使用条件情報を検査する手段を備え、使用条件が満たされない場合には上記鍵情報記憶手段が記憶している復号鍵を破棄することを特徴とする請求項１に記載のデジタルソフトウェア配布システム。

【請求項６】　上記使用条件には上記配付デジタルソフトウェアの利用回数が含まれており、

上記デジタルソフトウェアの受信側は、上記復号鍵の使用回数を記憶する手段を備え、

上記復号鍵の使用回数が上記使用条件として設定されている利用回数に達したことが検知された場合には、この復号鍵を破棄することを特徴とする請求項５に記載のデジタルソフトウェア配布システム。

【請求項７】　上記デジタルソフトウェアの受信側はさらに、上記復号手段により復号された配布デジタルソフトウェアを物理的な形に再生する再生手段を備え、

上記再生手段が上記配付デジタルソフトウェアの再生に失敗した場合には、上記復号鍵の使用回数を増やさないことを特徴とする請求項６に記載のデジタルソフトウェア配布システム。

【請求項８】　上記デジタルソフトウェアの受信側は、

上記復号鍵および上記復号鍵の使用回数を複数個記憶する手段と、

上記複数の復号鍵毎に識別子を設定する手段と、

上記設定した復号鍵の識別子を記憶する手段と、

上記識別子を外部に公開する手段と、

上記識別子から対応する復号鍵およびその復号鍵の使用回数を求める手段とを備え、

上記デジタルソフトウェアの配付側は、上記公開された識別子を受け取る手段と、

上記受信した識別子を配付デジタルソフトウェアに添付する手段とを備え、

上記デジタルソフトウェアの受信側は、上記配付デジタルソフトウェアに添付された識別子から対応する復号鍵およびその復号鍵の使用回数を求め、この求めた復号鍵の使用回数により復号鍵の破棄を行うとともに、この求めた復号鍵によって上記配付デジタルソフトウェアの復号を行うことを特徴とする請求項５～７の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項９】　上記復号鍵の識別子としてこの復号鍵に対応する暗号鍵を使用し、上記暗号鍵を公開する手段により上記識別子を公開する手段に代えることを特徴とする請求項４または８に記載のデジタルソフトウェア配布システム。

【請求項１０】　上記デジタルソフトウェアの配付側と受信側との間が通信回線で接続されており、上記通信回線によって上記暗号鍵、上記識別子および上記デジタルソフトウェアの伝送を行うこと特徴とする請求項１～９

の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項１１】　公開鍵暗号方式を用い、上記暗号鍵として公開鍵を使用するとともに、上記復号鍵として秘密鍵を使用することを特徴とする請求項１～１０の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項１２】　公開鍵暗号方式と共通鍵暗号方式とを併用し、上記暗号鍵として公開鍵を使用するとともに、上記復号鍵として秘密鍵を使用し、

上記暗号化手段によるデジタルソフトウェアの暗号鍵での暗号化が、上記デジタルソフトウェアを共通鍵で暗号化する手順と、上記共通鍵を上記暗号鍵で暗号化する手順と、暗号化した共通鍵を暗号化したデジタルソフトウェアに添付する手順とによって行われ、

上記復号手段によるデジタルソフトウェアの復号鍵での復号化が、デジタルソフトウェアに添付されている暗号化された共通鍵を求める手順と、求めた共通鍵を上記復号鍵で復号化する手順と、復号化した共通鍵で上記デジタルソフトウェアを復号化する手順とで行われることを特徴とする請求項１～１０の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項１３】　上記デジタルソフトウェアの受信側は、受信側固有の情報を持ち、この受信側固有の情報を公開する手段を備え、

上記デジタルソフトウェアの配付側は、上記受信側固有の情報を受け取って記憶する手段を備え、

配布者が配布デジタルソフトウェアを利用する側を特定することが可能なように構成されることを特徴とする請求項１～１２の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項１４】　上記受信側固有の情報がデジタル署名であることを特徴とする請求項１３に記載のデジタルソフトウェア配布システム。

【請求項１５】　請求項１１の公開鍵暗号方式、あるいは請求項１２の公開鍵暗号方式と共通鍵暗号方式とを併用したシステムであって、

上記デジタルソフトウェアの受信側は、上記受信側固有の情報あるいは上記デジタル署名を上記秘密鍵によって暗号化する手段を備え、

上記デジタルソフトウェアの配付側は、上記受信側固有の情報あるいは上記デジタル署名を上記公開鍵によって復号化する手段を備えることを特徴とする請求項１３または１４に記載のデジタルソフトウェア配布システム。

【請求項１６】　上記デジタルソフトウェアの配付側は、配布可能なデジタルソフトウェアの情報を公開する手段を備え、

上記デジタルソフトウェアの受信側は、上記配布可能なデジタルソフトウェアの情報を受け取る手段と、

上記配布可能なデジタルソフトウェアの情報を利用者に提示する手段と、

上記提示された情報の中から利用者が配布希望のデジタルソフトウェアを選択するための手段と、

上記選択されたデジタルソフトウェアを上記デジタルソフトウェアの配付側に通知する手段とを備えることを特徴とする請求項１～１５の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項１７】　上記デジタルソフトウェアの受信側は、利用者から使用料金の課金情報を受け取る手段と、受け取った課金情報を上記デジタルソフトウェアの配付側に通知する手段とを備え、

上記デジタルソフトウェアの配付側は、上記課金情報を受け取る手段と、

受け取った課金情報の正当性を確認する手段と、

上記課金情報をもとに使用料を徴収する手段とを備え、

利用者が有料のデジタルソフトウェアの配布を受けるときには利用者から課金情報を受け取ることで使用料金の徴収を行うようにしたことを特徴とする請求項１６に記載のデジタルソフトウェア配布システム。

【請求項１８】　上記課金情報が利用者のクレジットカード番号であることを特徴とする請求項１７に記載のデジタルソフトウェア配付システム。

【請求項１９】　上記課金情報が電子マネーであることを特徴とする請求項１７に記載のデジタルソフトウェア配付システム。

【請求項２０】　上記デジタルソフトウェアの受信側は、上記復号手段により復号された配布デジタルソフトウェアを物理的な形に再生する再生手段と、

上記再生手段の機能に関する情報を上記デジタルソフトウェアの配付側に通知する手段とを備え、

上記デジタルソフトウェアの配付側は、上記再生機能に関する情報を受け取る手段と、

受け取った再生機能に関する情報から最適なデジタルソフトウェアを選択する手段とを備えることを特徴とする請求項１～１９の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項２１】　上記デジタルソフトウェアの受信側は、上記復号手段により復号された配布デジタルソフトウェアを物理的な形に再生する再生手段と、

上記再生手段の機能に関する情報を上記デジタルソフトウェアの配付側に通知する手段とを備え、

上記デジタルソフトウェアの配付側は、上記再生機能に関する情報を受け取る手段と、

受け取った再生機能に関する情報をもとに、配布するデジタルソフトウェアを上記再生機能に関する情報に合う形に加工する手段とを備えることを特徴とする請求項１～１９の何れか１項に記載のデジタルソフトウェア配布システム。

【請求項２２】　暗号鍵によって暗号化されたデジタルソフトウェアを復号化するための上記暗号鍵に対応した復号鍵を記憶する鍵情報記憶手段と、

上記鍵情報記憶手段に記憶されている復号鍵を決められたタイミングで破棄する鍵情報破棄手段とを備えたことを特徴とする端末装置。

【請求項２３】　上記鍵情報記憶手段が記憶している復号鍵を破棄するタイミングは、上記デジタルソフトウェアを復号し終えたことに応じて決定されることを特徴とする請求項２２に記載の端末装置。

【請求項２４】　上記復号鍵によって復号されたデジタルソフトウェアを物理的な形に再生する再生手段を更に備え、

上記鍵情報記憶手段が記憶している復号鍵を破棄するタイミングは、上記復号されたデジタルソフトウェアを物理的な形に正常に再生し終えたことに応じて決定されることを特徴とする請求項２２に記載の端末装置。

【請求項２５】　上記暗号化されたデジタルソフトウェアに添付されている使用条件情報を検査する手段を更に備え、使用条件が満たされない場合に上記鍵情報記憶手段が記憶している復号鍵を破棄することを特徴とする請求項２２に記載の端末装置。

【請求項２６】　上記使用条件には上記デジタルソフトウェアの利用回数が含まれており、上記復号鍵の使用回数が上記使用条件として設定されている利用回数に達した場合に上記鍵情報記憶手段が記憶している復号鍵を破棄することを特徴とする請求項２５に記載の端末装置。

【請求項２７】　暗号鍵によって暗号化されたデジタルソフトウェアを復号化するための上記暗号鍵に対応した復号鍵を記憶手段に記憶する機能と、

上記記憶手段に記憶されている復号鍵を決められたタイミングで破棄する機能とをコンピュータに実現させるためのプログラム記録したコンピュータ読み取り可能な記録媒体。

【請求項２８】　請求項２７に記載の機能に加え、上記暗号化されたデジタルソフトウェアに添付されている使用条件情報を検査し、使用条件が満たされない場合に上記記憶手段に記憶されている復号鍵を破棄する機能をコンピュータに実現させるためのプログラム記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタルソフトウェア配布システム、端末装置および記録媒体に関し、特に、デジタル化されたあるいは初めからデジタルデータとして作成されたデジタルソフトウェアをネットワークを介して遠隔地の端末に配布し、利用者が配布されたソフトウェアのデジタルデータを物理的な形に再生して使用することが可能なデジタルソフトウェアの配布システムに用いて好適なものである。

【０００２】

【従来の技術】近年、音声・静止画・動画・文章などの各種ソフトウェアをデジタル化する技術が発達している。一方、プログラム言語やワープロ文書あるいはコンピュータグラフィックスのように、初めからデジタルデータとして作成されるソフトウェアも数多く存在している。

【０００３】これらのデジタルソフトウェアは、複製・伝送・保管などの操作によっても品質の劣化が起こらないという特徴を持つ。このため、通信回線を用いた安価な流通コストでの配布が可能であり、実際に現在、パソコン通信やインターネットなどでデジタルソフトウェアの配布サービスが行われている。

【０００４】しかし、ソフトウェア自体が無体財産としての価値を持つ著作物などの場合には、著作権を有する者の利益を守るために、ソフトウェアの不正な複製を防止する必要がある。そのため、通信回線を介してデジタルソフトウェアを配付するシステムを構築する場合に、複製が容易であるというデジタルソフトウェアの特徴が問題になっている。

【０００５】これに対して、デジタルソフトウェアを不正な複製等から保護するための技術として、データの暗号化がある。この技術は、利用者に対して暗号化したデータを配布するようにし、配布データを特定の利用者あるいは特定の装置でのみ利用できるようにすることにより、配布したデジタルソフトウェアの不正な流通を防ぐものである。

【０００６】

【発明が解決しようとする課題】しかしながら、従来の暗号化を使用した技術の多くは、流通途中で第三者によるデジタルソフトウェアの不正複製があった場合に、その複製デジタルソフトウェアを使用不可能にすることを目的としたものであった。そのため、正当に配布ソフトウェアを受け取った利用者がその配布ソフトウェアを複製した場合には、複製デジタルソフトウェアの不正利用を阻むことは難しい。

【０００７】このような利用者による複製デジタルソフトウェアの不正利用を防止する技術としては、特開平７－１３１４５２号あるいは特開平８－１１１６７１号などの発明が開示されているが、これらの技術では、配布者は契約を行った利用者に対して暗号解読装置または暗号解読用の鍵をあらかじめ渡しておく必要がある。そのため、配布者側は利用者に渡した鍵に関する情報を登録・管理する必要があり、不特定多数の顧客に対するソフトウェアの配布技術としては利用できない。

【０００８】また、特開平７－１３１４５２号に記載された発明では、公開暗号鍵を利用することによって鍵管理・配送が容易になるとしているが、具体的な内容については触れられていない。

【０００９】本発明は、このような実情に鑑みて成されたものであり、配布デジタルソフトウェアの不正使用の防止のうち、特に利用者が暗号化された配布デジタルソフトウェアの複製を不正に保持し、この暗号を解読する

ことができる装置を使用して繰り返し利用することを有効に防止できるようにすることを目的としている。

【００１０】さらにまた、配布者と利用者との間に事前の契約などを必要とせず、利用者が本システムに対応した装置を使用している限り、本システムに対応した不特定多数の配布者からデジタルソフトウェアの配布を受けられるようにすることをもう一つの目的としている。

【００１１】

【課題を解決するための手段】本発明では、例えば１つ以上のデジタルソフトウェア配付側装置と、１つ以上のデジタルソフトウェア受信側装置とによってシステムを構成する。デジタルソフトウェアの配布を行う者は配布側装置を使用し、デジタルソフトウェアを利用する者は受信側装置を使用する。

【００１２】第１の発明では、受信側装置内部で復号鍵と暗号鍵とを生成し、復号鍵は秘匿した状態で受信側装置の内部に記憶し、暗号鍵を配布側装置に渡す。配布側装置では、受け取った暗号鍵でデジタルソフトウェアを暗号化してから配布を行い、受信側装置は暗号化された状態で配布されたデジタルソフトウェアを上記記憶しておいた復号鍵で復号化するが、この復号鍵を決められたタイミングで破棄することにより、この復号鍵で復号可能であった配布デジタルソフトウェアの利用を終了するようにすることを特徴とする。

【００１３】ここで、暗号鍵および復号鍵は、暗号鍵をもとにデータの暗号化を行うと復号鍵を用いてこの暗号データを復号化することができるが、暗号鍵を用いてこの暗号データを復号化することはできず、暗号鍵から復号鍵を求めることもできないという関係を持つ暗号用の鍵である。

【００１４】このように構成した第１の発明によれば、利用者は受信側装置内部に復号鍵が記憶されている間は配布デジタルソフトウェアを復号して利用することができるが、受信側装置内部の復号鍵が破棄されると、配布デジタルソフトウェアを復号できなくなる。つまり、配布されたデジタルソフトウェアデータは、利用者が複製したデータを含め、受信側装置内部に復号鍵が記憶されている間だけそのソフトウェアとしての価値を持つことを保証する。このため配布者は、受信側装置が復号鍵を破棄するタイミングを決めておくことで、配布デジタルソフトウェアの価値を保つことが可能となり、また利用者は、あらかじめ配布者との間に契約を結ぶことなく、配布者にソフトウェアの配布を求めることが可能となる。

【００１５】第２の発明では、デジタルソフトウェアを復号したことに応じて受信側装置は復号鍵を破棄する。このように構成した第２の発明によれば、配布デジタルソフトウェアが一度だけ復号されることが保証される。

【００１６】第３の発明では、復号された配付デジタルソフトウェアを物理的な形に正常に再生し終えたことに応じて受信側装置は復号鍵を破棄する。これにより、受信側装置がデジタルソフトウェアの再生に失敗した場合でも、利用者は再び配布者にデジタルソフトウェアの配布を求めることなく、デジタルソフトウェアをもう一度再生することができる。

【００１７】第４の発明では、受信側装置は、複数の復号鍵を記憶する手段とこれらの復号鍵毎に設定した識別子を記憶する手段とを持つ。また、配付側装置は、公開された識別子を暗号化したデジタルソフトウェアに添付して配付する手段を持つ。受信側装置は、配布されたデジタルソフトウェアに添付された識別子をもとに、記憶している複数の復号鍵から復号する配付デジタルソフトウェアに必要な復号鍵を検索し、この復号鍵で配付デジタルソフトウェアの復号化を行う。これにより、利用者が一度に複数のデジタルソフトウェアの配布を受け、その中から好きな順番でデジタルソフトウェアの復号化を行うことが可能になる。

【００１８】第５の発明では、配付側装置は配布するデジタルソフトウェアに配布者が決定した使用条件情報を添付し、受信側装置はデジタルソフトウェアに添付された使用条件が満たされない場合に復号鍵を破棄し、デジタルソフトウェアの復号を行えないようにする。これにより、配布者は配布するデジタルソフトウェアの使用条件を配布時に決定することができるようになる。

【００１９】第６の発明では、第５の発明において利用回数を配付デジタルソフトウェアの使用条件とするものであり、受信側装置が復号鍵の使用回数をカウントすることで、復号鍵の使用回数とデジタルソフトウェアに添付された利用回数とを比べて使用条件の判定とする。これにより、配布者は配布するデジタルソフトウェアの利用回数を配布時に決定することができるようになる。

【００２０】第７の発明では、第６の発明において受信側装置が配付デジタルソフトウェアの再生に失敗した場合には復号鍵の使用回数を増やさないようにする。これにより、受信側装置が配付デジタルソフトウェアの再生に失敗した場合でも、利用者は再び配布者にデジタルソフトウェアの配布を求めることなく、デジタルソフトウェアを配布者の設定した利用回数だけ再生することができる。

【００２１】第８の発明では、第４の発明に加え、受信側装置が複数の復号鍵の利用回数を記憶する手段を持つ。受信側装置は、配布されたデジタルソフトウェアに添付された識別子をもとに、記憶している複数の復号鍵から復号する配付デジタルソフトウェアに必要な復号鍵とその利用回数とを検索し、利用回数で使用条件を判定して復号鍵の破棄を行うとともに、復号鍵で配付デジタルソフトウェアの復号化を行う。これにより、配布者が使用条件を配付時に設定することができ、なおかつ、利用者が一度に複数のデジタルソフトウェアの配布を受け、その中から好きな順番でデジタルソフトウェアの復

号化を行うことが可能になる。

【００２２】第９の発明では、受信側装置の公開する暗号鍵を、第４の発明または第８の発明における識別子として使用する。これにより、受信側装置が配布側装置に渡す情報を、暗号鍵と識別子との２つから暗号鍵だけに減らすことができる。

【００２３】第１０の発明では、受信側装置と配布側装置の間を通信回線で接続し、この通信回線で暗号鍵、識別子およびデジタルソフトウェアの伝送を行う。これにより、例えばＴＣＰ／ＩＰ（transmission control protocol / internet protocol）やＨＴＴＰ（hyper text transfer protocol）やＦＴＰ（file transfer protocol）などの既存のデータ通信プロトコルを本発明のシステムに使用し、インターネットやイントラネットあるいは公衆電話回線などの既存のインフラを利用した安価なシステムを構築することができる。

【００２４】第１１の発明では、暗号方式に公開鍵暗号方式を用い、配付側装置の暗号鍵として公開鍵を使用するとともに、受信側装置の復号鍵として秘密鍵を使用する。これにより、例えばＲＳＡ方式などの普及した方式を取り入れて、既存の暗号化装置や復号化装置を本システムの一部として使用することが可能になり、システム開発を容易にすることができる。

【００２５】第１２の発明では、暗号方式に公開鍵暗号方式と共通鍵暗号方式とを併用し、配布側装置がデジタルソフトウェアを暗号化する際に大部分のデータは共通鍵暗号方式で暗号化し、共通鍵の情報を含む一部のデータのみを公開鍵暗号方式により暗号化する。共通鍵は暗号鍵によって暗号化された状態でデジタルソフトウェアに添付され、受信側装置に渡される。これにより、公開鍵暗号方式の暗号化処理および復号化処理の速度を速くするために高価な装置を導入することなく、共通鍵暗号化方式による安価な装置で暗号化および復号化の大部分の処理速度を上げることができ、システム全体の処理速度を向上させることができる。

【００２６】第１３の発明では、受信側装置が受信側に固有の情報を持っており、これを暗号鍵や識別子と共に配布側装置に渡す。これにより、配布者および配布側装置は、複数の受信側の中から配布デジタルソフトウェアを利用する受信者または受信側装置を特定することができる。

【００２７】第１４の発明では、第１３の発明における受信側固有の情報をデジタル署名とするものである。ここで、認証変数を必要とするデジタル署名方式を用いる場合は、配布側装置あるいはデジタル署名の認証サーバから受信側装置に認証変数が渡され、この認証変数をもとに受信側装置がデジタル署名を作成して配布側装置に渡す。これにより、例えば配布側装置が認証サーバにデジタル署名の認証を依頼することで、受信側装置が認証サーバに登録されたものであることを証明することができる。このため、本発明のシステムに対応した受信側装置だけを登録する認証サーバを作り、受信側装置のメーカが出荷する受信側装置のデジタル署名を全て登録することで、配布側装置に配布要求を行う受信側装置が本発明のシステムに対応したものであることを保証できる。

【００２８】第１５の発明では、第１１の発明あるいは第１２の発明による暗号方式を採用し、受信側装置が第１３の発明における受信側固有の情報または第１４の発明におけるデジタル署名を配布側装置に送るときに、配布側装置にデジタルソフトウェアの暗号鍵として送る公開鍵に対応する秘密鍵で暗号化しておく。配布側装置は、受け取った公開鍵で受信側固有の情報またはデジタル署名の復号化を行う。これにより、配布側装置は、暗号鍵として受け取った公開鍵と受信側固有の情報またはデジタル署名とが、同じ受信側装置から送られてきたものであることを確認することができ、利用者が本システムに対応した装置のデジタル署名とそれ以外の公開鍵とを組み合わせる不正を見破ることができる。

【００２９】第１６の発明では、配布側装置が配布可能なデジタルソフトウェアの情報を公開しており、受信側装置が上記配布可能なデジタルソフトウェアの情報を利用者に提示し、利用者がその中から希望するデジタルソフトウェアを選択すると、受信側装置が選択されたソフトウェアの配布を配布側装置に要求する。これにより、配布者が配布側装置を公開する作業を行うだけで、利用者は複数の配布側装置の中から好きなソフトウェアの配布を受けることができる。

【００３０】第１７の発明では、受信側装置が利用者から課金情報を受け取り、その課金情報を配布側装置に渡し、配布側装置が受け取った課金情報の正当性を確認した上でこの課金情報をもとに配布するソフトウェアの代金を徴収する。これにより、配布者はデジタルソフトウェアの配布に伴う収入を得ることが可能になる。

【００３１】第１８の発明では、第１７の発明による課金情報として利用者のクレジットカード番号を使用する。これにより、配布者は新たな料金徴収システムを開発することなく、クレジットカード会社の構築するシステムで料金の徴収が行え、利用者はクレジットカードさえ持っていれば本システムを利用することができる。

【００３２】第１９の発明では、第１７の発明による課金情報として電子マネーを使用する。これにより、配布者は新たな料金徴収システムを開発することなく、電子マネーを扱う会社の構築するシステムで料金の徴収が行え、利用者は電子マネーさえ持っていれば本システムを利用することができる。

【００３３】第２０の発明では、配布側装置が１つのソフトウェアに関して受信側装置の種類や再生方法別にデジタルデータを複数保持しており、受信側装置がデジタルソフトウェアの再生に関する情報を配布側装置に渡し、配布側装置はこの情報から最適なデジタルデータを

選択してデジタルソフトウェアとして配布する。これにより、受信側装置の種類が複数存在しても、利用者の持っている受信側装置とその装置の状態に合わせたデジタルデータを配布することが可能になる。

【００３４】第２１の発明では、受信側装置が配付されたデジタルソフトウェアの再生に関する情報を配布側装置に渡し、配布側装置はこの情報をもとにデジタルソフトウェアのデジタルデータを加工してから配布する。これにより、第２０の発明において、デジタルソフトウェアのデータのうち受信側装置の種類によって変化する部分があまり多くない場合に、配布側装置が同じようなデジタルデータを複数保持する必要がなくなる。

【００３５】

【発明の実施の形態】以下に、本発明の実施の形態を、具体的な例を用いて詳細に説明する。

【００３６】（第１の実施形態）本実施形態では、本発明によるデジタルソフトウェア配布システムの一実施形態として、電子出版システムの例を示す。本実施形態による電子出版システムでは、配布者である出版社が配布処理装置を使用し、利用者である読者が再生装置を使用する。また、配布するデジタルソフトウェアは、画像や文書のデータや、ページ記述言語や構造化言語などから構成される出版データであり、利用者は配布されたデジタルソフトウェアを紙に印刷して利用する。

【００３７】図１は、本実施形態による電子出版システムの概略図である。図１に示すように、本実施形態による電子出版システムでは、１台以上の配布処理装置１０００と１台以上の再生装置２０００とがネットワーク３０００によって接続されている。ネットワーク３０００は、データを双方向に伝送可能であれば任意だが、例えばインターネットを利用することで、世界中で利用可能な電子出版システムを安価に提供することができる。

【００３８】図２は、本発明におけるシステムの配布処理装置１０００の一構成例を示すブロック図である。図２に示すように、配布処理装置１０００は、認証機関の端末１１００とクレジットカード会社の端末１２００と接続されている。ネットワーク３０００としてインターネットを利用する場合には、認証機関１１００およびクレジットカード会社１２００との接続も、インターネットを経由して行うことが可能である。

【００３９】この配布処理装置１０００は、出版データ１００４として配布する電子出版物を格納しており、注文受注部１００１と、課金処理部１００２と、認証処理部１００３と、出版データ取り出し部１００５と、暗号化処理部１００６と、配布出版データ送信部１００７とを備えている。これら各部の動作については後で詳しく説明する。

【００４０】図３は、本発明におけるシステムの再生装置２０００の一構成例を示すブロック図である。この再生装置２０００は、ＰＣ（パソコン）２１００とプリンタ２２００とから構成されており、プリンタ２２００は、鍵生成部２２０１、鍵情報記憶部２２０２、デジタル署名部２２０３、復号部２２０４、検証部２２０５、内蔵時計２２０６および印刷部２２０７を備えている。プリンタ２０００の内部の動作は、一般の利用者に対して機密が保たれるようになっている。

【００４１】図４のフローチャートに、ＰＣ２１００に設定された動作手順の一例を示す。この動作は、ＰＣ２１００のＯＳ上で動くアプリケーションプログラムや、WWW（world wide web）ブラウザ上で動作するスクリプトや、WWWブラウザの補助プログラムなどの形態で実現することが可能である。

【００４２】図４において、まず利用者から配布処理装置１０００の指定（電子出版物の配付元の選択）を受け付け（ステップＳ１）、この指定された配布処理装置１０００から出版目録を受け取る（ステップＳ２）。次に、出版目録の中の購入する電子出版物の注文を利用者から受け付ける（ステップＳ３）。そして、注文した電子出版物の代金の支払いを行うクレジットカード番号の入力を利用者から受け付ける（ステップＳ４）。

【００４３】ここで、電子出版物の印刷を行うプリンタ２２００の情報を取得するように指示すると（ステップＳ５）、プリンタ２２００の鍵生成部２２０１が公開鍵暗号方式の秘密鍵と公開鍵とを作り、秘密鍵はプリンタ内部の鍵情報記憶部２２０２とデジタル署名部２２０３とに渡され、公開鍵はＰＣ２１００に渡される。鍵情報記憶部２２０２は、鍵生成部２２０１から渡された秘密鍵を記憶し、さらに秘密鍵の使用回数として０回を記憶する。

【００４４】また、デジタル署名部２２０３は、デジタル署名を生成し、受け取った秘密鍵でこのデジタル署名を暗号化する。そして、この暗号化したデジタル署名を鍵生成部２２０１からの公開鍵と共にＰＣ２１００に渡す。デジタル署名方式として認証変数が必要な方式で行う場合には、認証機関１１００あるいは配布処理装置１０００から認証変数を取り寄せ、これをプリンタ２２００のデジタル署名部２２０３に渡してデジタル署名の作成を行う。

【００４５】次にＰＣ２１００は、利用者の選択した電子出版物の指定（注文）情報と、プリンタ２２００から受け取った公開鍵およびデジタル署名と、利用者が入力したクレジットカード番号とが揃ったら、これらを指定した配布処理装置１０００に送信する（ステップＳ６）。配布処理装置１０００は、これらの情報を受け取ると該当する電子出版物データの送信処理を行うが、この処理については後で詳しく述べる。

【００４６】その後、指定した配布処理装置１０００から電子出版物データが送られてくると、このデータをＰＣ２１００内の記憶部にファイルとして保存する（ステップＳ７）。そして、受け取った電子出版物を印刷する

ために、ファイルとして保存した電子出版物データをプリンタ２２００に送る（ステップＳ８）。もし、プリンタ２２００がジャムなどを起こして印刷が正常に行われなかった場合には、ファイルとして保存した電子出版物データをもう一度プリンタ２２００に送り、印刷を実行する作業を繰り返す（ステップＳ９）。

【００４７】また、後述のように秘密鍵の複数回の使用が許されている場合には、その回数の正常な印刷が行われるまで印刷を実行する作業が繰り返される。最後に、許された回数の印刷が正常に実行され、不必要になった電子出版物データファイルをＰＣ２１００内の記憶部から削除する（ステップＳ１０）。

【００４８】次に、図５のフローチャートに配布処理装置１０００の受注処理の動作手順の一例を示す。図５において、配布処理装置１０００の注文受信部１００１は、電子出版物の注文に必要なデータとして、再生装置２０００側で利用者の選択した電子出版物の指定情報と、プリンタ２２００からＰＣ２１００が受け取った公開鍵およびデジタル署名と、利用者が入力したクレジットカード番号とを再生装置２０００から受け取る（ステップＳ１０１）。

【００４９】これらの情報を受け取ったら、注文受信部１００１はまず最初に、指定された電子出版物を持っているかどうかを調べる（ステップＳ１０２）。注文が有効であれば次に、課金情報が有効かどうかを課金処理部１００２に問い合わせる（ステップＳ１０３）。課金処理部１００２は、クレジット会社１２００に対して、利用者のクレジットカード番号のチェックを依頼し、その結果を注文受信部１００１に返す。

【００５０】課金情報が有効であった場合にはさらに、注文受信部１００１はデジタル署名が有効かどうかを認証処理部１００３に問い合わせる（ステップＳ１０４）。認証処理部１００３は、デジタル署名を公開鍵で復号化し、復号化したデジタル署名が認証機関１１００に登録されているかを調べ、登録されている情報を受け取る。デジタル署名が登録されているならば、このデジタル署名と暗号鍵（秘密鍵）とが登録されている再生装置２０００で注文が作成されたことを意味する。

【００５１】クレジットカード番号およびデジタル署名のチェックで問題が起きなければ、出版データ取り出し部１００５によって、注文を受けた電子出版物を出版データ１００４の格納部から取り出す（ステップＳ１０５）。また、認証機関１１００に登録されている情報として、発注を行った利用者のプリンタ２２００の情報が登録されているため、このプリンタ情報から、使用するページ記述言語の種類あるいは印字可能色数や解像度などの情報を求め、プリンタ２２００にとって最適なデータを取り出すようにする。

【００５２】なお、電子出版物データのうち再生装置２０００の種類によって変化する部分があまり多くない場合には、基本となる電子出版物データのみを登録しておき、プリンタ情報をもとにプリンタ２２００にとって最適なデータとなるように電子出版物データを加工するように構成しても良い。

【００５３】これらのデータが取り出せたならば、暗号化処理部１００６が公開鍵により配付出版データの暗号化を行い、その後暗号化に使用した公開鍵とこの公開鍵で暗号化した使用条件とを添付する（ステップＳ１０６）。配付出版データの使用条件は、配布者があらかじめ設定しておく。最後に、暗号化したデータを配布出版データ送信部１００７が利用者のＰＣ２１００に送信し（ステップＳ１０７）、最後まで正常に送信が行えたならば（ステップＳ１０８）、課金処理部１００２がクレジット会社１２００に代金の請求を行う（ステップＳ１０９）。

【００５４】次に、図６のフローチャートに再生装置２０００内のプリンタ２２００の電子出版物印刷処理の動作手順の一例を示す。図６において、ＰＣ２１００内の記憶部から暗号化された電子出版物データが渡されると（ステップＳ２０１）、復号部２２０４は、この暗号化された電子出版物データに添付されている公開鍵と使用条件とを取り出し、この公開鍵と使用条件とを検証部２２０５に渡す（ステップＳ２０２）。

【００５５】検証部２２０５は、渡された公開鍵に対応する秘密鍵とこの秘密鍵の使用回数とを鍵情報記憶部２２０２から捜し出す（ステップＳ２０３）。公開鍵に対応する秘密鍵とこの秘密鍵の使用回数とが記憶されていれば（ステップＳ２０４）、秘密鍵の使用回数および内蔵時計２２０６の日時と使用条件とを比較する（ステップＳ２０５）。

【００５６】ここで、もし使用条件が満たされていなければ（ステップＳ２０６）、鍵情報記憶部２２０２に記憶されているこの秘密鍵と秘密鍵の使用回数とを削除する（ステップＳ２０７）。もし使用条件を満たしていれば（ステップＳ２０６）、検証部２２０５は秘密鍵を復号部２２０４に返し、復号部２２０４はこの秘密鍵によって電子出版物データの復号化を行う（ステップＳ２０８）。

【００５７】そして、復号化した電子出版物データを印刷部２２０７に送り、印刷を実行する（ステップＳ２０９）。印刷時にジャムなどが発生せずに正常に印刷を終了できた場合には（ステップＳ２１０）、鍵情報記憶部２２０２に記憶されている秘密鍵の使用回数を１つ増加させて処理を終了する（ステップＳ２１１）。一方、印刷時にジャムなどが発生して正常に印刷ができなかった場合には（ステップＳ２１０）、秘密鍵の使用回数は増やさずに処理を終了する。なお、複数回の使用が許可されている場合には、再び、ＰＣ２１００内の記憶部から暗号化された電子出版物データを取り出し（ステップＳ２０１）、この図６のフローチャートに従う処理をその

回数繰り返す。

【００５８】以上の説明から明らかなように、本実施形態の電子出版システムを用いれば、配布者は不特定多数の利用者に対して電子出版物の配布を行い、その際に配布電子出版物の使用条件を設定できるとともに、利用者から使用料を徴収することができ、利用者による不正使用を有効に防ぐことができる。例えば、配付者側で電子出版物の使用回数を制限する使用条件を設定することにより、利用者が配布された電子出版物の複製を不正に保持し、それを使用条件を越えて繰り返し利用することを有効に防止することができる。

【００５９】また、利用者は本システムに対応した再生装置を用意することで、事前に契約や登録を行うことなく、任意の配布処理装置から電子出版物を購入したり配布を受けたりして、配布された電子出版物を利用することができる。

【００６０】なお、以上の実施形態では、配付者によって決められた利用回数を電子出版物の使用条件として設定し、復号鍵の使用回数が使用条件として設定されている利用回数に達した場合に再生装置２０００が記憶している復号鍵を破棄するようにしたが、使用回数の条件を１回に固定しておき、配付電子出版物の復号が終わった時点で復号鍵を破棄するようにしても良い。この場合には、配布された電子出版物データを一度だけ復号して利用可能なようにすることができる。

【００６１】また、再生装置２０００が記憶している復号鍵を破棄するタイミングは、配布された電子出版物データを復号して正常に印刷し終えたときとしても良い。この場合には、再生装置２０００で電子出版物の印刷に失敗した場合でも、利用者は再び配布者に電子出版物の配布を求めることなく、当該電子出版物をもう一度印刷することができる。

【００６２】また、上記実施形態では、１つの再生装置２０００では１つの秘密鍵を記憶することを前提としているが、複数の秘密鍵を記憶するように構成しても良い。この場合には、各秘密鍵毎に識別子を設定して識別子も記憶する。配付処理装置１０００は、再生装置２０００から識別子を受け取り、その受信した識別子を電子出版物データに添付して配付する。配付を受けた再生装置２０００では、添付された識別子から対応する秘密鍵を求め、この求めた秘密鍵によって上記配付デジタルソフトウェアの復号を行う。このように構成した場合には、利用者が一度に複数の電子出版物の配布を受け、その中から好きな順番で電子出版物の再生を行うことが可能になる。

【００６３】さらに、上述の秘密鍵に加えて、再生装置２０００において秘密鍵の使用回数情報も複数個記憶するように構成しても良い。この場合、配布された電子出版物データに添付されている識別子をもとに、対応する秘密鍵とその使用回数情報とを検索し、識別子に対応する使用回数情報で使用条件を判定して秘密鍵の破棄を行う。このように構成した場合には、利用者が一度に複数の電子出版物の配布を受け、その中から好きな順番で電子出版物の再生を行う際に、再生する電子出版物毎に配布者が使用条件を設定することができる。なお、上述の識別子は、秘密鍵に対応する公開鍵であって良い。

【００６４】また、上記実施形態では、暗号方式として公開鍵暗号方式を採用しているが、公開鍵暗号方式と共通鍵暗号方式とを併用しても良い。この場合、電子出版物データを暗号化する際に、大部分のデータは配布処理装置１０００内で生成した共通鍵で暗号化し、共通鍵の情報を含む一部のデータのみを公開鍵により暗号化する。そして、上述の共通鍵は、公開鍵によって暗号化した状態で電子出版物データに添付し、再生装置２０００に送信する。このように構成した場合には、共通鍵暗号方式による安価な装置で暗号化および復号化の大部分の処理速度を上げることができ、システム全体の処理速度を向上させることができる。

【００６５】また、上記実施形態ではデジタル署名を用いているが、再生装置２０００に固有の情報であれば、配布者は複数の再生装置１０００の中から電子出版物データを利用する再生装置を特定することができ、正当に利用可能な者であるかどうかを確認することができるので、デジタル署名以外の情報であっても良い。また、上述の実施形態では、課金システムとしてクレジット会社を介在させたシステムを説明したが、電子マネーを利用した課金システムとしても良い。

【００６６】また、以上の実施形態では、デジタルソフトウェア配布システムの一例として電子出版システムを考え、復号化した配付デジタルソフトウェアを印刷する場合について説明したが、本発明はこれに限定されない。すなわち、配付するデジタルソフトウェアは電子出版物データ以外のものであっても良く、配付デジタルソフトウェアの再生方法も印刷以外の方法であっても良い。もちろん、復号したデジタルソフトウェアをコンピュータ画面上で利用するだけのものにも適用することが可能である。

【００６７】また、図３に示したプリンタ２２００の内部構成のうち、印刷部２２０７以外の構成はＰＣ２１００内に設けても良い。

【００６８】（本発明の他の実施形態）本発明は、上述した実施形態の機能を実現するように各種のデバイスを動作させるように、該各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００６９】また、この場合、上記ソフトウェアのプロ

グラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００７０】また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

【００７１】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【００７２】

【発明の効果】本発明は上述したように、デジタルソフトウェアの受信側で復号鍵と暗号鍵とを生成し、このうち公開した暗号鍵によって配布側で暗号化され配布されたデジタルソフトウェアを受信側において上記復号鍵で復号化する構成において、生成した復号鍵を受信側に記憶しておき、それをその後決められたタイミングで破棄するようにしたので、受信側に復号鍵が記憶されている間だけ配布デジタルソフトウェアを復号して利用することができ、復号鍵が破棄された後は配布デジタルソフトウェアを復号できなくなるようにすることができる。これにより、配布者は不特定多数の利用者に対してデジタルソフトウェアの配布を行い、例えば復号鍵を破棄するタイミングを決めておくことで、利用者による不正使用を防ぐことができる。また、利用者は本システムに対応した装置を用意することで、事前に配付者と契約や登録を行うことなく、任意の配布側装置からデジタルソフトウェアの購入や配布を受けて、配布されたデジタルソフトウェアを利用することができる。

【００７３】また、本発明の他の特徴によれば、デジタルソフトウェアの配付側で配付するデジタルソフトウェアに関して使用条件情報を添付する手段を設け、デジタルソフトウェアの受信側でその使用条件が満たされない＊と判断した場合に上記復号鍵を破棄するようにしたので、配付者が配布デジタルソフトウェアの使用条件を配布時に設定することができる。例えば、使用条件として配布デジタルソフトウェアの利用回数を設定した場合には、受信側では設定された使用条件の回数を越えて配布デジタルソフトウェアを繰り返し利用できないようにできる。

【００７４】また、本発明のその他の特徴によれば、デジタルソフトウェアの受信側で利用者から使用料金の課金情報を入力して配付側に通知するようにしたので、デジタルソフトウェアの配付者は利用者から使用料を徴収することが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態である電子出版システムの概略構成を示すブロック図である。

【図２】本発明の一実施形態である電子出版システムにおける配布処理装置の概略構成を示すブロック図である。

【図３】本発明の一実施形態である電子出版システムにおける再生装置の概略構成を示すブロック図である。

【図４】本発明の一実施形態である電子出版システムにおけるＰＣの動作手順を示すフローチャートである。

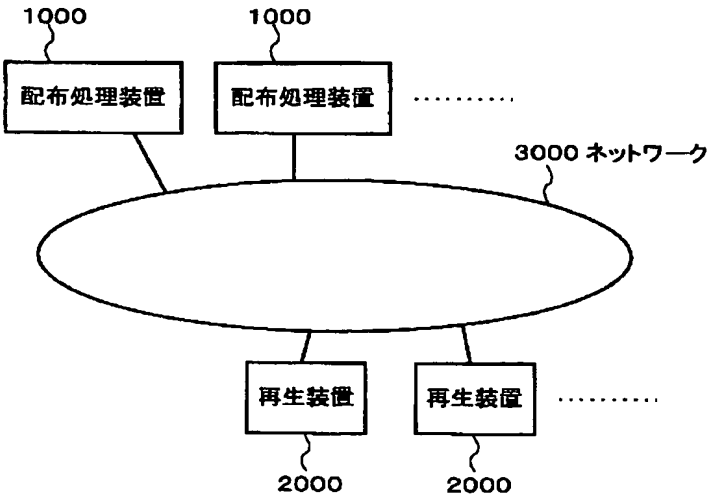
【図５】本発明の一実施形態である電子出版システムにおける配布処理装置の配布処理手順を示すフローチャートである。

【図６】本発明の一実施形態である電子出版システムにおけるプリンタの印刷手順を示すフローチャートである。

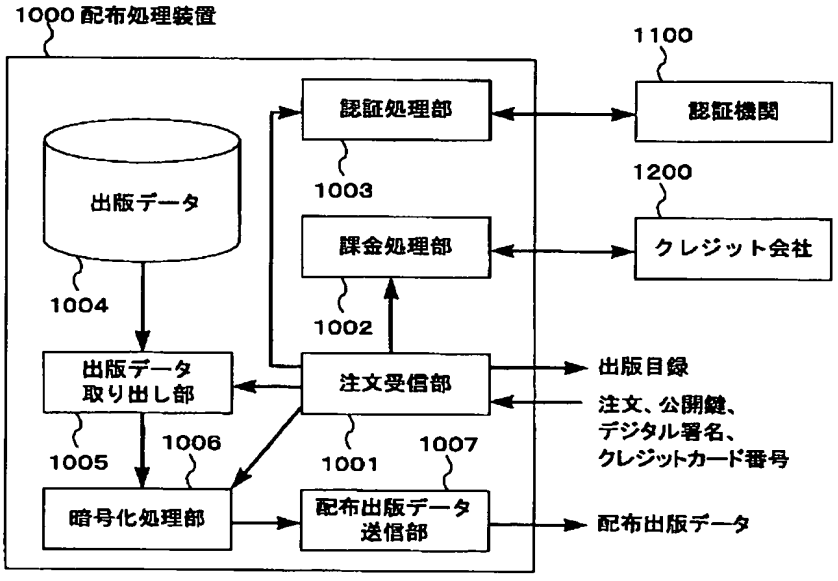
【符号の説明】

１０００　配付処理装置
１００１　注文受信部
１００２　課金処理部
１００３　認証処理部
１００４　出版データ
１００５　出版データ取り出し部
１００６　暗号化処理部
１００７　配付出版データ送信部
２０００　再生装置
２１００　ＰＣ
２２００　プリンタ
２２０１　鍵生成部
２２０２　鍵情報記憶部
２２０３　デジタル署名部
２２０４　復号部
２２０５　検証部
２２０６　内蔵時計
２２０７　印刷部

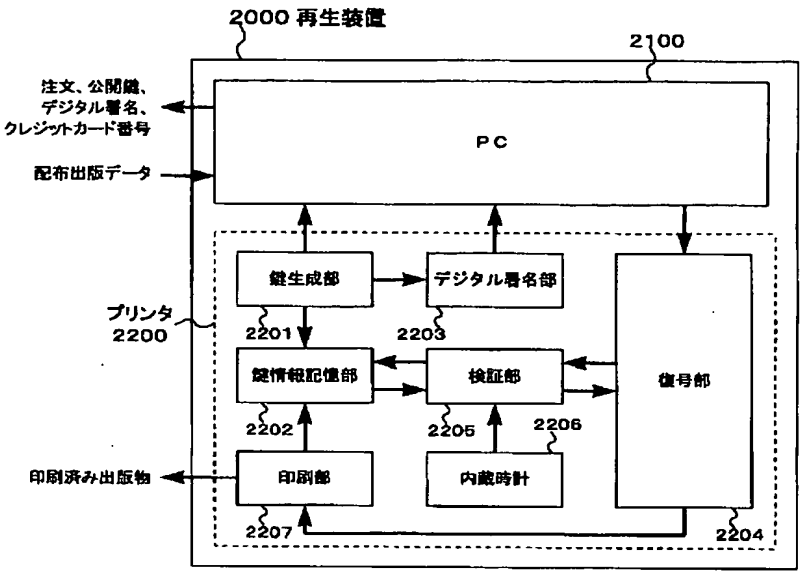
【図１】


1000
1000
配布処理装置
配布処理装置
3000 ネットワーク
再生装置
再生装置
2000
2000

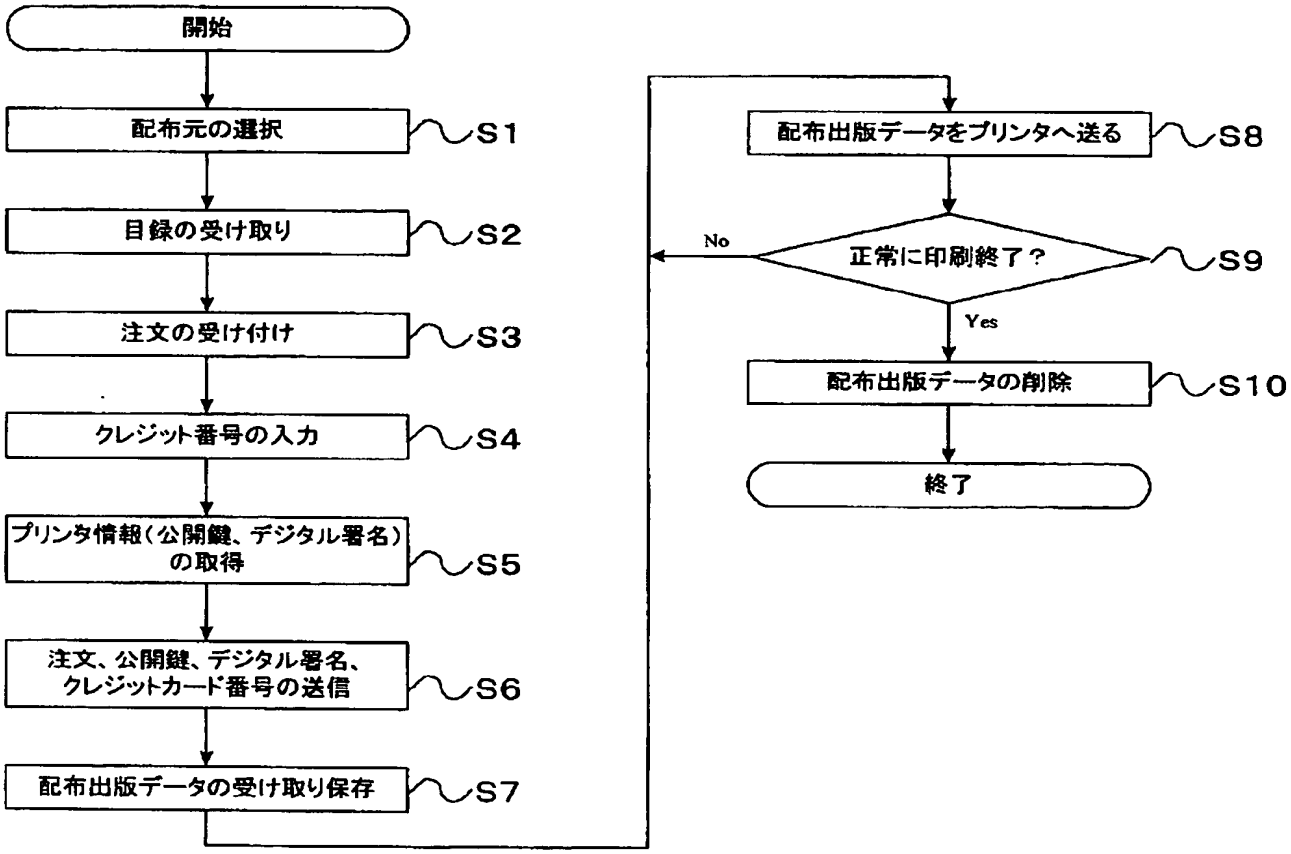
【図２】


1000 配布処理装置
1100
認証処理部
認証機関
出版データ
1003
1200
課金処理部
クレジット会社
1004
1002
出版データ
取り出し部
注文受信部
出版目録
注文、公開鍵、
デジタル署名、
クレジットカード番号
1005
1006
1001
1007
暗号化処理部
配布出版データ
送信部
配布出版データ

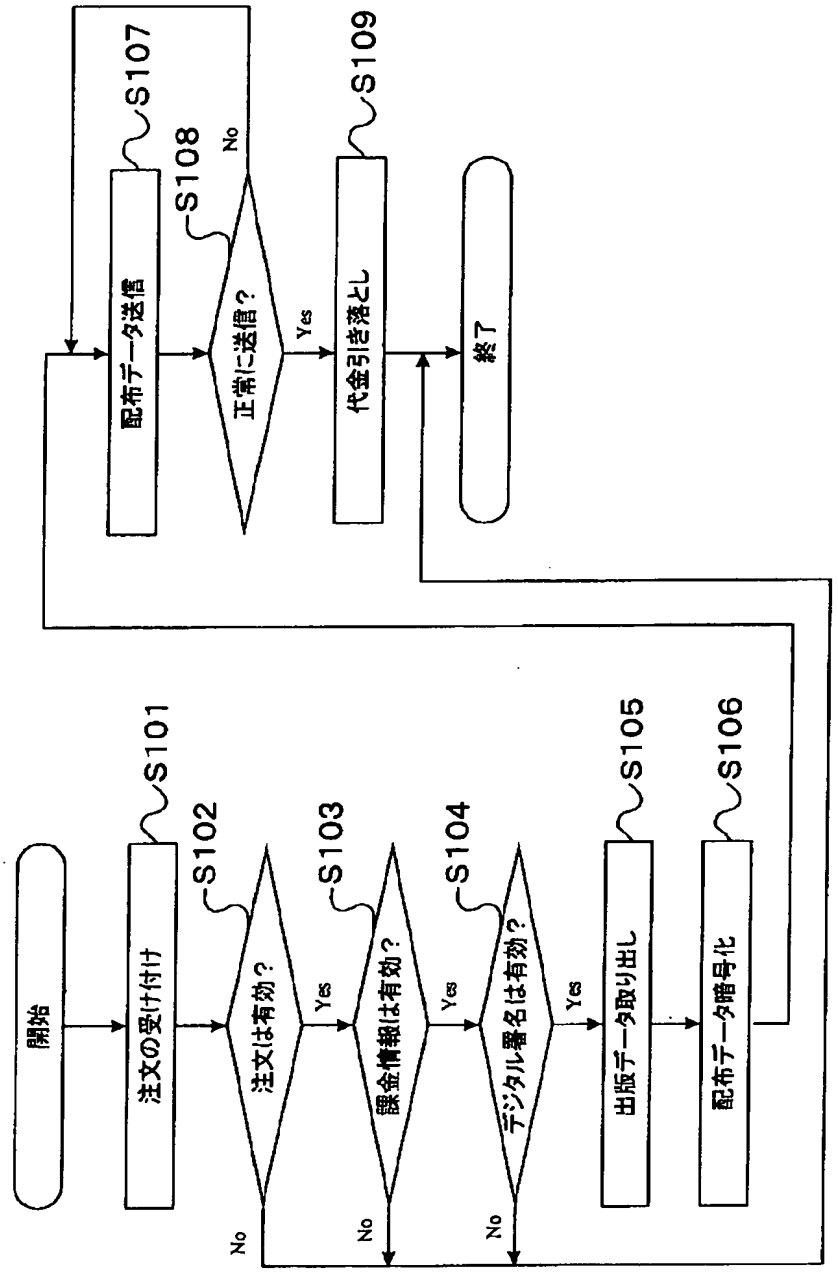
【図３】


2000 再生装置
2100
注文、公開鍵、
デジタル署名、
クレジットカード番号
配布出版データ
PC
鍵生成部
デジタル署名部
プリンタ
2200
2201
2203
鍵情報記憶部
検証部
復号部
2202
2205
2206
印刷済み出版物
印刷部
内蔵時計
2207
2204

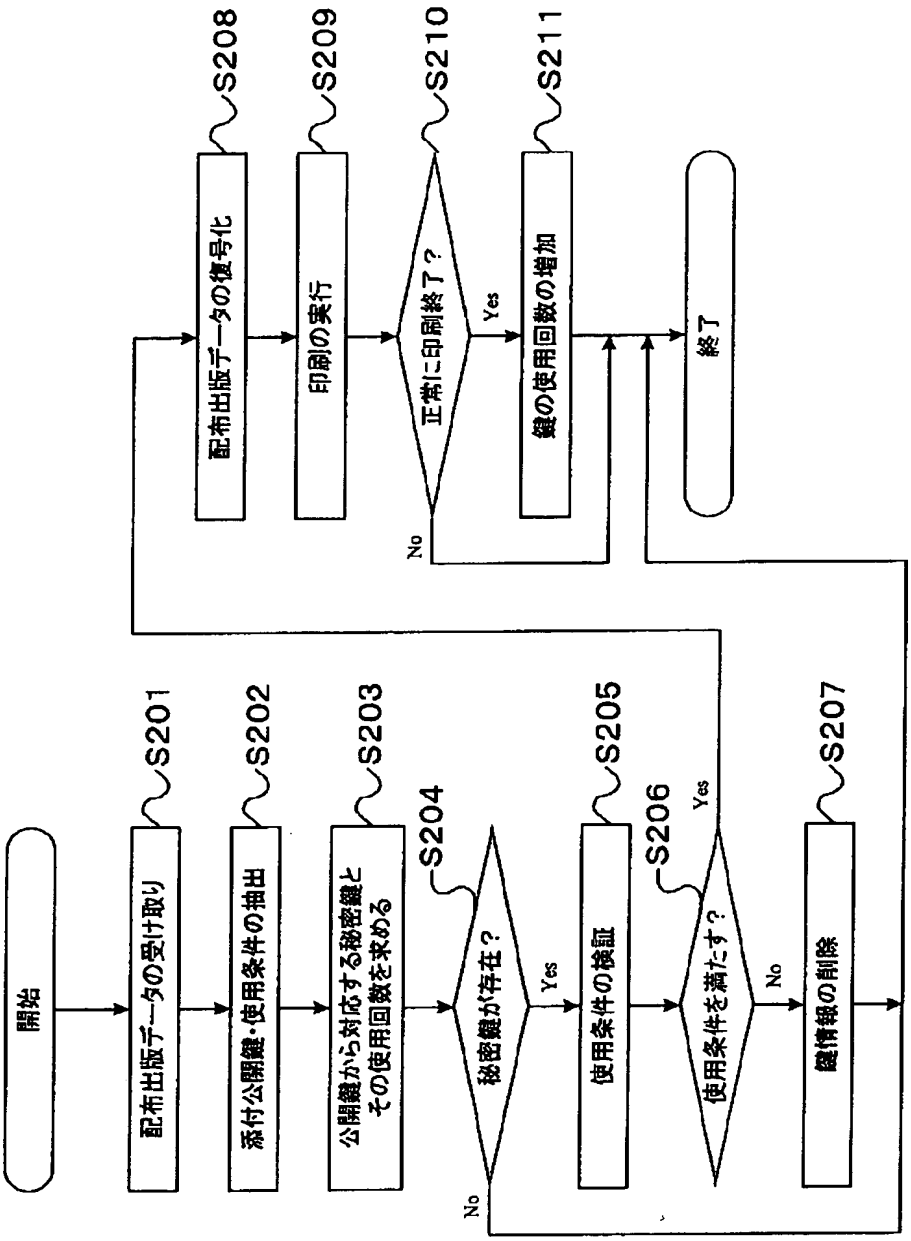
【図４】


開始
配布元の選択
S1
目録の受け取り
S2
注文の受け付け
S3
クレジット番号の入力
S4
プリンタ情報（公開鍵、デジタル署名）
の取得
S5
注文、公開鍵、デジタル署名、
クレジットカード番号の送信
S6
配布出版データの受け取り保存
S7
配布出版データをプリンタへ送る
S8
No
正常に印刷終了？
S9
Yes
配布出版データの削除
S10
終了

【図５】


開始
注文の受け付け
S101
注文は有効？
S102
No
Yes
課金情報は有効？
S103
No
Yes
デジタル署名は有効？
S104
No
Yes
出版データ取り出し
S105
配布データ暗号化
S106
代金引き落とし
S109
終了
配布データ送信
S107
正常に送信？
S108
No
Yes

【図６】


開始
S201
配布出版データの受け取り
S202
添付公開鍵・使用条件の抽出
S203
公開鍵から対応する秘密鍵とその使用回数を求める
S204
秘密鍵が存在？
Yes
No
S205
使用条件の検証
S206
使用条件を満たす？
Yes
No
S207
鍵情報の削除
S208
配布出版データの復号化
S209
印刷の実行
S210
正常に印刷終了？
Yes
No
S211
鍵の使用回数の増加
終了